

XML DATA ENCODING SPECIFICATION FOR NEED-TO-KNOW METADATA VERSION 2

ICTechSpec 500.D.4-V2

An Intelligence Community Technical Specification
Prepared by the
Intelligence Community Chief Information Officer

7 September 2010



Table of Contents

Table of Contents	i
List of Figures	iii
List of Tables	iii
Chapter 1 – Introduction	1
1.1 Purpose	1
1.2 Needs and Requirements	1
1.3 Audience and Applicability	2
1.4 Utility	2
1.5 Version Information	2
1.6 Components of this DES	3
1.7 Normative and Informative Components	3
1.8 Technical Encoding Dependencies	4
1.9 Typographic conventions	4
Chapter 2 – Development Guidance	5
2.1 Mapping of Abstract Data Elements to Physical XML Elements	5
2.2 Additional Guidance	6
2.2.1 <i>Integration into a schema</i>	6
2.2.2 <i>Basic usage model</i>	6
2.2.3 <i>Guidance for the specification of constraints for a particular access system</i>	7
2.2.4 <i>Guidance for systems processing data containing NTK metadata</i>	7
Chapter 3 – XML Schema Guide	9
Chapter 4 – Data Validation Constraint Rules	10
4.1 Basics	10
4.1.1 <i>"Living" Constraint Rules</i>	10
4.1.2 <i>Classified or Controlled Constraint Rules</i>	11
4.1.3 <i>Terminology</i>	11
4.1.4 <i>Rule Identifiers</i>	11
4.1.5 <i>Errors and Warnings</i>	11
4.2 Conditions	12
4.2.1 <i>Conditions</i>	12
4.3 Global Constraints	12
4.3.1 <i>DES Constraints</i>	13
4.4 Validation Against External Controlled Value Enumerations	13
4.5 General Constraints	13
4.6 Obsolete rule numbers	13
Appendix A IC CIO Approval Memo	14
Appendix B Acronyms	15
Appendix C Glossary	17
Appendix D Bibliography	18
Appendix E Points of Contact	21

Appendix F	Change History	22
Appendix G	Configuration Management	23
Appendix H	Reading the Schematics	24
H.1	Element Models	24
H.2	Groupings of Elements	25
H.3	Occurrence indicators.....	26
H.4	Order of Elements.....	27
H.5	Attributes	28
Appendix I	Controlled Vocabulary Enumerations	29

List of Figures

Figure 1. Symbol for an XML Element having Element Content.....	24
Figure 2. Symbol of an Element with Mixed Content.....	25
Figure 3. Symbol of an Empty Element.....	25
Figure 4. Element Group Symbol.....	26
Figure 5. Optional elements, one repeatable, graphical representation	26
Figure 6. Optional and repeatable element, graphical representation.....	27
Figure 7. Required and repeatable element, graphical representation.....	27
Figure 8. Sequence Symbol	27
Figure 9. Choice Symbol.....	28
Figure 10. Sequence and Choice Combined	28

List of Tables

Table 1. DES change summary	3
Table 2. Mapping of Abstract Data Elements to Physical XML Elements	5
Table 3. DES Version Identifier History	22
Table 4. CVE Definitions	29

Chapter 1 – Introduction

1.1 Purpose

This *XML Data Encoding Specification for Need-To-Know Metadata* (NTK.XML) defines detailed specifications for using Extensible Markup Language (XML) to encode metadata necessary to facilitate automated systems making a “need-to-know” (NTK) determination in order to access information. This Data Encoding Specification (DES) defines the XML elements and attributes; associated structures and relationships; mandatory and cardinality requirements; and permissible values for representing (NTK) metadata associated with an information resource or part of an information resource using XML.

These metadata are used to represent the system-specific properties assigned to an information resource that will be used, in conjunction with information about the user, and possibly other information, to determine the user’s access to the data. A single information resource may include multiple occurrences of these metadata in order to specify (NTK) information according to multiple, different access systems. Each of the access systems will provide the specifics about the metadata to be captured. See **Section 2.2** for more information on the use of these metadata.

1.2 Needs and Requirements

Information sharing within the national intelligence enterprise frequently relies on being able to determine an individual’s need-to-know as one component in determining whether to allow access to data. The enterprise will increasingly rely on need-to-know metadata to allow users and systems to find and access a wide-range of data throughout the enterprise. A successful information sharing enterprise depends on the ability of the data creator and or providers to specify the means by which need-to-know can be established in a manner to facilitate discovery and access via automated means.

This DES provides a common specification for the means by which a data producer can encode, in their data, the information an access system needs to determine how to grant access. This DES enables a comprehensive capability that can appropriately protect data across the enterprise while also allowing access by individuals having appropriate need-to-know. The nature of the information to be encoded will vary system by system and could include lists of individuals or groups permitted access, descriptions of subject matter in terms defined by the access system, or other traits to be used in evaluating the access an individual has to the data.

This DES provides that common specification. Currently the particulars of any access system's data needs are not defined. Details for specifying access information and documenting access parameters for particular access systems are to be added in the near future. The systems for which access information will be recorded and constrained will be expanded as their applicability's are identified to the enterprise.

1.3 Audience and Applicability

DESs are intended primarily to be used by those developing tools and services to create, modify, store, exchange, search, display, or further process the type of data being described. The applicability and conditions for when the DES should be used will be found in the *Intelligence Community Standards Registry* (ICSR) when established, and in approved IC policy guidance written specifically to address information sharing objectives in the context of particular intelligence functions, intelligence information, and desired data formats. Policy would include but not be limited to ICD 206, ICD 500, ICD 501, ICD 710, ICPG 501.1, ICPG 501.2, Controlled Access Program Coordination Office (CAPCO), Register and Implementation Manual, Information Security Oversight Office (ISOO) Directive 1, Executive Order (E.O.) 13526, and E.O. 12829.

1.4 Utility

A DES specifies how to implement the abstract concepts defined in the *IC Abstract Data Definition* (IC.ADD) in a particular physical form (e.g., data or file format). For example:

- DESs for textual markup formats, such as XML and HyperText Markup Language (HTML), define markup elements and attributes, their relationships, cardinalities, processing requirements, and use.
- DESs for display formats, such as text and Adobe Portable Document Format (PDF), define text and typographic conventions, cardinalities, processing requirements, and use.
- DESs for application-specific formats, such as Microsoft Word, define document properties, styles, fields, cardinalities, processing requirements, and use.

1.5 Version Information

This is **Version 2** of this DES. This version number must be specified in the **DESVersion** attribute within any XML instance document claiming to be valid against this version. A separate **DESVersion** attribute must be specified for each DES against which an instance document is claiming compliance. These attributes must be in the namespace specified by each DES.

The following table lists the major changes made to this DES.

Table 1. DES change summary

Change	Artifacts changed	Compatibility Notes
Use ISM V4	Schema	Data generation and Ingestion systems need to be updated to properly enforce the new constraint rule
Use Schema to enforce DES version number	NTK-ID-00003	Data Ingestion systems need to be updated to use the new Schema instead of constraint rules.

1.6 Components of this DES

This document is the primary documentary component of the DES. This document contains:

- **Chapter 1 – Introduction.** The introduction describes high-level background information for this document. It defines the purpose and scope of this document.
- **Chapter 2 – Development Guidance.** This chapter covers two primary topics:
 - 1) Mappings of the XML element and attributes defined within this DES to appropriate IC.ADD data elements
 - 2) Descriptions of how particular encoding situations should be handled using the features provided by this DES
- **Chapter 3 – XML Schema Guide.** Highlights the availability of an interactive presentation of the PUBS.XML schema as well as an implementation-specific data element dictionary.
- **Chapter 4 – Data Validation Constraint Rules.** The constraint rules in this chapter define data validation constraints for PUBS.XML beyond those in the XML Schema.

1.7 Normative and Informative Components

The XML schema is normative for this DES. Additionally, an access system may specify that certain CVE values and constraint rules are normative for data to be processed by

that system. The rest of this document, the descriptive content referenced within the XML Schema Guide, and example files are informative.

1.8 Technical Encoding Dependencies

This DES relies on access systems to specify how the specific values are to be encoded in order to support their functioning. The information to be provided by access systems includes value enumerations and constraint rules. This information will be recorded in the appropriate component of this DES.

1.9 Typographic conventions

Certain typography is used throughout the body of this document to convey certain meanings, in particular:

- *Italics* – A title of a referenced work or a specialized or emphasized term.
- Underscore – An abstract data element.
- **Bold** – An XML element or attribute.

Chapter 2 – Development Guidance

This chapter covers two primary topics:

- 1) Mappings of the XML element and attributes defined within this DES to appropriate IC.ADD data elements
- 2) Descriptions of how particular encoding situations should be handled using the features provided by this DES

2.1 Mapping of Abstract Data Elements to Physical XML Elements

The mapping of abstract data elements from the IC.ADD to the corresponding physical XML structures defined by this DES is shown in the following tables, which reflect the groupings in the IC.ADD. These mappings are provided for reference only. The complete set of DES artifacts, both normative and informative, should be consulted.

This mapping and additional mappings in other DESs provide a starting point for the development of automated transformations between formats defined by the DESs. However, it should be noted that when these transformations are used between formats with different levels of detail, there might be some data loss.

Table 2. Mapping of Abstract Data Elements to Physical XML Elements

Abstract Data Element	Definition	XPath and XML implementation notes
Access Expression	A statement or description of a group of people who should be granted access to an information resource.	//Access
Access individual	A statement, as defined by an access system, of a mechanism that identifies an individual who has access to the resource.	//AccessIndividual
Access group	A statement, as defined by an access system, of a group that should refer ultimately to one or more individuals.	//AccessGroup
Access parameter	A statement of the traits that an access system will use in determining if a particular individual making a request for access to an information resource is granted access.	//AccessProfile

2.2 Additional Guidance

2.2.1 Integration into a schema

In order to use the capabilities of this DES, the XML schema that is part of this DES must be incorporated into another XML schema to be useful. For purposes of this documentation, we will refer to this other schema as the "resource" schema. Additionally, the "resource" schema must include the XML schema of the XML Data Encoding Specification for Information Security Marking (ISM.XML). The basic process for incorporation is as follows:

- Import this schema in to "resource" schema
- Define a namespace prefix
- Allow for the **DESVersion** attribute to be used in the "resource" schema
- Ensure (Information Security Marking Metadata) ISM is incorporated into the "resource" schema
- Add the Access element to the "resource" schema model at an appropriate location

The specification is designed to record NTK information for an entire resource to include the NTK information itself. This means that those that have access to the resource will have access to all of the NTK information.

2.2.2 Basic usage model

In order for this DES to be effectively implemented in the enterprise, the following usage model description should be used.

First, an access system that wishes to provide access control services to the enterprise must define the parameters they need to make decisions and/or the specific syntax by which individuals and/or groups are referenced. This information should also be published and made accessible to those who created resources and who wish to control access to those resources via that system. These specifications can be documented as per **Section 2.2.3**.

Next, the creators of resources who wish to control access to their resources via one of these access systems must specify the access to the resource using the specifics defined by the desired access system. The resource creator can decide to specify access in terms of more than one access system.

This DES is initially published without specifying CVE's or many constraint rules. It is expected that as enterprise systems are recognized and adopt this model the CVE's and constraints will be fleshed out. The expectation is to have a small number of enterprise access systems.

2.2.3 Guidance for the specification of constraints for a particular access system

When an access system desires to use the capabilities of this DES to document how information concerning access should be specified by resource producers, they shall abide by the following guidelines.

- The access system owner shall provide a name for the system to be used in the CVE for the element **AccessSystemName**.
- The access system owner shall provide a syntax, pattern, or CVE for the elements **AccessIndividualValue**, **AccessGroupValue**, and **AccessProfileValue**.
- The access system owner shall provide guidance on encoding, in the syntax of this DES, for all parameters necessary to be specified on the resource, other than those encoded via ISM.

Depending on the data format for the resource, data used for access control, may be duplicated; one instance in the resource's usual encoding, the other in the access model. The benefit of this possible duplication is that the explicit specification of the access information in a consistent manner allows for resources to implement this DES in multiple different schemas' that may locate the duplicate information in many different elements or attributes.

2.2.4 Guidance for systems processing data containing NTK metadata

It is important to note that data may have multiple access system requirements expressed (e.g., system A profile, system B profile, etc.). Each system is to be considered separately. This means that the set of people or systems having access to the data is the union of the people or systems described by the NTK metadata supplied for all access systems.

Systems handling data containing NTK metadata must assess and understand the NTK metadata in order to protect the data appropriately. A best practice for addressing this issue is to first examine any NTK metadata that may exist within the data being received. If NTK metadata is present, the receiving system should look for NTK

metadata expressed in terms of an access system it understands. If no understandable NTK metadata is located, the files should be segregated and protected via the most restrictive manner available, and the submitter should be contacted to understand any possible ramifications.

Chapter 3 – XML Schema Guide

The detailed description and reference documentation for the NTK.XML schema can be found in a separate document entitled *NTK.XML Schema Guide*. This guide serves as an interactive presentation of the NTK.XML schema as well as a data element dictionary.

The guide was generated with a commercially available product named *XML Spy®*, produced by Altova. The physical XML structures illustrated in the guide are described in **Appendix H**.

The guide provides an interactive index to:

- Global Elements and Attributes
- Local Elements and Attributes
- Simple and Complex Types
- Groups and Attribute Groups
- Referenced Schemas

Where applicable, the guide provides:

- Diagram
- Namespace
- Type
- Children
- Used by
- Properties
- Patterns
- Enumerations
- Attributes
- Annotations
- Source Code

The guide is published in a folder consisting of a master HTML file with supporting graphics.

Chapter 4 – Data Validation Constraint Rules

Constraint Rules explicitly define the validation constraints for NTK.XML. They provide additional restrictions (i.e., constraints) on how the data should be structured and encoded especially for criteria that exceed the constraints implemented in the XML Schema. These rules are written in plain English phrases; however, knowledge of the NTK.XML schemas is required to understand the rules. These constraint rules will eventually be offered in a more declarative form, such as Schematron. Complex constraint rules may be followed by text labeled **Human Readable**. This text is intended to inform the intent of the more formal language above it. Implementers are intended to implement the formal language, and should there be a perception of conflict, bring it to the attention of the appropriate configuration control body to be resolved.

4.1 Basics

The NTK.XML schema defines the data elements, attributes, cardinalities, and parent-child relationships for which XML instances must comply. Validation of these syntax aspects is an important first step in the validation process. An additional level of validation is needed to ensure that the content complies with the constraints as specified in applicable Intelligence Community (IC) policy guidance and codified in these constraint rules. Traditional schema languages are generally unable to effectively represent these additional constraints.

4.1.1 “Living” Constraint Rules

These constraint rules are a "living" rule set. The constraint rules provided below are a valid starter set and do not attempt to address the full scope of access systems which may leverage this DES. Providers of access systems using this DES are encouraged to work with the maintainers of this DES to ensure that their system-specific constraints are appropriately documented in this document and/or other appropriate artifacts.

Since these constraint rules are only a subset of the entire rule base, an XML document that is compliant with these rules may still not be fully compliant with all of the business rules defined in the authoritative guidance. An XML document that is not compliant with these rules is not compliant with the authoritative guidance.

4.1.2 Classified or Controlled Constraint Rules

Additional rules that are either classified or have handling controls can be found in separate annexes closely associated with the DES artifacts wherever they are located.

4.1.3 Terminology

For the purposes of this document, the following statements apply:

- The term “is specified” indicates that an attribute is applied to an element and the attribute has a non-null value.
- The term “must be specified” indicates that an attribute must be applied to an element and the attribute must have a non-null value.
- The term “is not specified” indicates that an attribute is not applied to an element, or an attribute is applied to an element and the attribute has a null value.
- The term “must not be specified” indicates that an attribute must not be applied to an element.

4.1.4 Rule Identifiers

Each constraint rule has an assigned rule ID, indicated in brackets preceding the constraint rule description. The rule IDs from 00001 to 10000 are unclassified and 10001 to 20000 are “for official use only” (FOUO). IDs from 20001 to 30000 are reserved for “Secret” rules and 30001 and above for more classified rules.

As the constraint rules are managed over time, IDs from deleted rules will not be reused.

4.1.5 Errors and Warnings

The severity of a constraint rule violation is categorized as either an “Error” or a “Warning.” An “Error” is naturally more severe and is indicative of a clear violation of an NTK.XML constraint rule, which would be likely to have a significant impact on the quality of a document. A “Warning” is less severe although noteworthy, and may not necessarily have any impact on the quality of a document. The severity of a constraint rule violation is indicated in brackets preceding each constraint rule description.

Each system responsible for processing a document (e.g., create, modify, transform, or exchange) must make a mission-appropriate decision about using a document with errors or warnings based on mission needs.

4.2 Conditions

Conditions are used to centralize some common criteria that apply to many constraint rules. They also allow for a change to impact many rules when there is a determination of error.

Human Readable: The element in the schema that represents the NTK values of the resource. Aggregator schemas might have multiple **ntk:Access** elements, access systems shall choose the first one in document order as the one to use for access to the entire resource.

4.2.1 Conditions

These conditions are used in many of the constraints to centralize conditions that apply to many rules.

[NTK-RESOURCE-ELEMENT][true/false] Return true if: The Element is the first **ntk:Access** element in document order.

Human Readable: The Element is the first **ntk:Access** element encountered in a depth-first traversal of the document elements from start to end.

4.3 Global Constraints

[NTK-ID-00001][Error] For every optional attribute that is used in a document, a non-null value must be present.

Human Readable: In other words, the attribute "is specified" as defined in **Section 4.1.3**.

4.3.1 DES Constraints

The DESVersion is specified through attributes on the root element. These attributes are constrained by the following rules. The **DESVersion** enables systems processing an instance document to be certain which set of constraint rules, schema, CVE's and business rules are intended by the author to be used.

4.4 Validation Against External Controlled Value Enumerations

CVE's for the access systems will be provided as they become available.

4.5 General Constraints

As systems provide them constraints for use will be provided.

[NTK-ID-00002][Error] **ntk:Access** must contain at least one of **ntk:AccessIndividualList**, **ntk:AccessGroupList**,**ntk:AccessProfileList**

Human Readable: In other words, to use NTK you have to specify at least one method.

4.6 Obsolete rule numbers

[NTK-ID-00003] Removed in V4

Appendix A IC CIO Approval Memo

An Office of the Intelligence Community Chief Information Officer (OCIO) Approval Memo should accompany this enterprise technical data specification bearing the signature of the Intelligence Community Chief Information Officer (IC CIO) or an IC CIO-designated official(s). If an OCIO Approval Memo is not accompanying this specification's version release package, then refer back to the authoritative web location(s) for this specification to see if a more complete package or a specification update is available.

Specification artifacts display a date representing the last time a version's artifacts as a whole were modified. This date most often represents the conclusion of the IC Element collaboration and coordination process. Once the IC Element coordination process is complete, the specification goes through an internal OCIO staffing and coordination process leading to signature of the OCIO Approval Memo. The signature date of the OCIO Approval Memo will be later than the last modified date shown on the specification artifacts by an indeterminable time period.

Upon signature of the OCIO Approval Memo, IC Elements may begin to use this specification version in order to address mission and business objectives. However, it is critical for IC Elements, prior to disseminating information encoded with this new specification version, to ensure that key enterprise services and consumers are prepared to accept this information. IC Elements should work with enterprise service providers and consumers to orchestrate an orderly implementation transition to this specification version in concert with mandatory and retirement usage decisions captured in the IC Enterprise Standards Baseline as defined in Intelligence Community Standard (ICS) 500-20.

Appendix B Acronyms

This appendix lists all the acronyms referenced in this DES and lists other acronyms that may have been used in other DES. This appendix is a shared resource across multiple documents so in any given DES there are likely acronyms that are not referenced in that particular DES.

CAPCO – Controlled Access Program Coordination Office

CVE – Controlled Vocabulary Enumeration

DCMI – Dublin Core Metadata Initiative

DC MES – Dublin Core Metadata Element Set

DES – Data Encoding Specification

DOI – Digital Object Identifier

DNI – Director National Intelligence

E.O. – Executive Order

GNS – Geographic Names Server

HTML – HyperText Markup Language

IC.ADD – Intelligence Community Abstract Data Definition

IC CIO – Intelligence Community Chief Information Officer

ICD – Intelligence Community Directive

ICS – Intelligence Community Standard

ISBN – International Standard Book Number

ISM – Information Security Marking Metadata

ISO – International Organization for Standardization

ISOO – Information Security Oversight Office

KA – Knowledge Assertion

KOS – Knowledge Organization System

MIME – Internet Media Types

NARA – National Archives and Records Administration

NGA – National Geospatial Intelligence Agency

NSI – National Security Intelligence

ODNI – Office of the Director of National Intelligence

SSC – Special Security Center

TGN – Thesaurus of Geographic Names

URI – Uniform Resource Identifier

URL – Uniform Resource Locator

W3CDTF – World Wide Web Consortium Date Time Format

XML – Extensible Markup Language

Appendix C Glossary

No pertinent glossary items requiring further definition.

Appendix D Bibliography

This appendix lists all the sources referenced in this DES and lists other sources that may have been used in other DES. This appendix is a shared resource across multiple documents so in any given DES there are likely sources that are not referenced in that particular DES.

(CAPCO Implementation Guide)

Intelligence Community Classification and Control Markings Implementation Manual. Unclassified FOUO version. Volume 3, Edition 1 (Version 3.1). 7 May 2010. Director of National Intelligence (DNI), Special Security Center (SSC), Controlled Access Program Coordination Office (CAPCO).

https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/CAPCO_Implementation%20Manual_FOUO_v3%201_07%20May%2010%20.pdf

(CAPCO Register)

Authorized Classification and Control Markings Register. Unclassified FOUO version. Volume 3, Edition 1 (Version 3.1). 7 May 2010. Director of National Intelligence (DNI), Special Security Center (SSC), Controlled Access Program Coordination Office (CAPCO).

[https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/CAPCO_Register_FOUO_v3%201_07%20May%2010%20\(2\).pdf](https://www.intelink.gov/sites/ssc/divisions/capco/CAPCO%20Resources/CAPCO_Register_FOUO_v3%201_07%20May%2010%20(2).pdf)

(DC MES)

Dublin Core Metadata Element Set. Version 1.1. 02 June 2003. Dublin Core Metadata Initiative. <http://dublincore.org/documents/dces/>.

(E.O. 12958, as amended)

Executive Order 12958 – Classified National Security Information, as Amended. Federal Register, Vol. 68, No. 60. 25 March 2003. The White House.

<http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html>.

(E.O. 12829, as amended)

Executive Order 12829 – National Industrial Security Program, as Amended. Federal Register, Vol. 58, No. 240. 16 December 1993. The White House.

<http://www.archives.gov/isoo/policy-documents/eo-12829.html>

(E.O. 13526)

Executive Order 13526 – Classified National Security Information 29 December 2009. The White House. <http://www.archives.gov/isoo/pdf/cnsi-eo.pdf>.

(ICD 206)

Sourcing Requirements for Disseminated Intelligence Products. Intelligence Community Directive Number 206. 17 October 2007. Office of the Director of National Intelligence. http://www.dni.gov/electronic_reading_room/ICD_206.pdf.

(ICD 500)

Director of National Intelligence Chief Information Officer. Intelligence Community Directive Number 500. 7 August 2008. Office of the Director of National Intelligence. http://www.dni.gov/electronic_reading_room/ICD_500.pdf.

(ICD 501)

Director of National Intelligence Chief Information Officer. Intelligence Community Directive Number 501. 21 January 2009. Office of the Director of National Intelligence. http://www.dni.gov/electronic_reading_room/ICD_501.pdf.

(ICD 710)

Classification and Control Markings System. Intelligence Community Directive Number 710. 11 September 2009. Office of the Director of National Intelligence. http://www.dni.gov/electronic_reading_room/ICD_710.pdf

(ISO 639-2)

Codes for the representation of names of languages – Part 2: Alpha-3 code. ISO 639-2:1998. International Organization for Standardization (ISO). http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=4767.

(ISO 3166-1)

Codes for the representation of names of countries and their subdivisions – Part 1: Country codes. ISO 3166-1:2006. International Organization for Standardization (ISO). http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39719.

(ISO 8601)

Data elements and interchange formats – Information interchange – Representation of dates and times. ISO 8601:2004. International Organization for Standardization (ISO). http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40874.

(ISO 15836)

Information and documentation – The Dublin Core metadata element set. ISO 15836:2009. International Organization for Standardization (ISO). http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=52142.

(ISOO Directive 1)

Classified National Security Information (Directive No. 1); Final Rule. 32 CFR Parts 2001 and 2004. Federal Register, Vol. 68, No. 183. 22 September 2003. Information Security Oversight Office (ISOO), National Archives and Records Administration (NARA). <http://www.archives.gov/isoo/policy-documents/eo-12958-implementing-directive.pdf>.

(RFC 3066)

Tags for the Identification of Languages. January 2001. H. Alvestrand. Cisco Systems. <http://www.rfc-editor.org/rfc/rfc3066.txt>.

Appendix E Points of Contact

This technical specification is managed by the Office of the Intelligence Community Chief Information Officer (IC CIO). As of this writing, the IC CIO/IC Enterprise Architecture (ICEA) Directorate facilitates the IC data collaboration and coordination forums responsible for the selection or development of common IC technical data specifications. Direct all inquiries about this IC technical specification to IC CIO/ICEA, the IC's data collaboration and coordination forum, or IC element representatives involved in those forums.

Appendix F Change History

The following table summarizes the version identifier history for this DES.

Table 3. DES Version Identifier History

Version	Identifier	Date	Purpose
1		11 May 2010	Initial Release
2		13 August 2010	Routine revision to technical specification. For details of changes, see section 1.5.

Appendix G Configuration Management

The selection or development of technical data specifications of common interest to the IC are collaborated and coordinated currently within governance forums managed by the IC CIO. Change requests for this technical data specification should be directed to the office identified in **Appendix E – Points of Contact**.

Appendix H Reading the Schematics

The physical XML structures documented in this guide are illustrated with schematics created with the commercially available product named *XML Spy®*, produced by Altova. The symbology used by *XML Spy®* is described in this appendix.

H.1 Element Models

In *XML Spy*, XML elements are represented by rectangles like that shown for an element named **PublicationMetadata** in **Figure 1**. XML elements may have one of three types of content model:

- Element content: A model in which the content consists entirely of child elements; in other words, there is no *direct* data content (although the child elements may have data content).
- Mixed content: A model in which the content consists of text, possibly intermixed with child elements; child elements in mixed content are said to float in the text in that their use is not constrained to a hierarchy.
- Empty: A model in which the element has no content; the element's function is performed by its attribute(s), if any, or the element is simply a placeholder for data that will be generated when the element is rendered for presentation.
-



Figure 1. Symbol for an XML Element having Element Content

An element whose model is element content is illustrated by the preceding figure. The "+" symbol in the small box at the right edge denotes that **PublicationMetadata** has content.

In the *XML Spy* graphical user interface (GUI), a schematic may be expanded and contracted to expose more or less of the model. In the GUI, clicking with the mouse on the "+" symbol causes the content of the element (in this case **PublicationMetadata**) to be revealed and the "+" is replaced by a "-" symbol. The purpose for pointing this out is that, in the remainder of this appendix, some of the illustrations show the "-" rather than the "+".

An element whose model is *mixed content* is represented by the symbol shown in **Figure 2**. As above, the "+" signifies that the element has content, and the lines in the upper left corner denote that text is allowed. Mixed content is the normal model for elements like paragraphs, list items, titles, *et al.*, in which the text "contains" semantic objects like footnote references, superscripts and subscripts, italicized and bolded passages, quoted strings, words or phrases that have been tagged for indexing or searching, *etc.* These types of semantic objects that appear in the running text are represented in XML as elements.



Figure 2. Symbol of an Element with Mixed Content

An *empty* element is illustrated by **Figure 3**. Note that the element symbol lacks a "+" symbol, meaning that content is not allowed. Empty elements do not have textual content. They are used for one or more of three possible purposes:

- They are pointers to text or non-text objects that are located in external files. In this capacity, they can be used as placeholders for illustrations. They mark the position where a graphic is to be placed and, using attributes, identify the file that contains the graphic image.
- They are placeholders for application-generated content that will be created as part of the rendering process. Examples include tables of contents, indexes, glossaries, and bibliographies. Empty elements are used to specify the positioning of such constructs.
- They mark locations that are acted upon by formatting engines. A common example is to use an empty element called **br** or **break** to tell a formatter to insert a newline sequence at the point where the empty element is encountered.



Figure 3. Symbol of an Empty Element

H.2 Groupings of Elements

XML Spy represents an XML schema element group that has been used in a content model with a rounded box. In **Figure 4**, **ComplexContentGroup** is the name of an element group.



Figure 4. Element Group Symbol

Note the use of the “+” symbol. In the GUI, clicking on this symbol reveals the composition of the element group. This is illustrated later on in this appendix.

H.3 Occurrence indicators

Some elements must be used, they are designated as required. Other elements are designated as optional. Both required and optional elements may be repeatable. These in combination make four classes of occurrence indicators: a required element that can be used once and only once, a required element that may repeat, an optional and repeatable element, and an optional element that may not repeat.

Figure 5 illustrates several elements the use of which is optional. The dotted border of the element symbols for **UUID**, **DocumentID**, and **InternalID** denote optionality. This means that the producer may use these elements to tag document identifiers, but their use is not required. The XML document will be deemed *syntactically* correct with or without them.

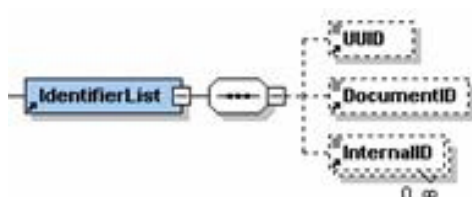


Figure 5. Optional elements, one repeatable, graphical representation

It is important to emphasize, in conjunction with **Figure 5**, that syntactic correctness and semantic completeness are distinct requirements. While an automated XML processing software application will accept element **IdentifierList** with or without the child elements, a production organization will need to apply local business rules to require at least one of the child elements to be present. This is done in order to allow the model to be used throughout the life cycle of the data. For example, the model can be used both at the time of authoring when the values for the child elements may not be known and later on when the values are required during the exchange with a partner.

The next two figures illustrate the symbols for repeatable elements. In **Figure 6**, element **InternalID** may be used zero or more times, as indicated by the “0..∞” string

beneath the symbol. Note also that a repeatable element is denoted by a stack of element symbols.

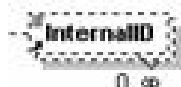


Figure 6. Optional and repeatable element, graphical representation

By contrast, in **Figure 7**, the element named **Section** must be used at least once, and may be used multiple times in succession. The fact that the section element symbol has solid borders means that its use is required. The "1..∞" beneath the symbol means it can be used one or more times.



Figure 7. Required and repeatable element, graphical representation

An element symbol that has solid borders and neither "0..∞" nor "1..∞" beneath must be used one and only one time. In **Figure 5**, the element named **IdentifierList** must be used once and only once.

H.4 Order of Elements

In many cases, XML schemas require that elements be used in a prescribed sequence. As shown in **Figure 8** this constraint is denoted by an ellipsis in a rounded box in the schematics:

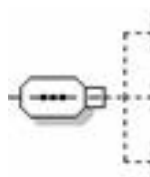


Figure 8. Sequence Symbol

The connecting lines leading from the right edge lead to three elements, which, if used, must be used in top-to-bottom order. **Figure 5** shows this symbol in a larger context. It says that the subelements of **IdentifierList** are all optional but, if used, must be in the order shown.

Figure 9 shows the symbol that signifies that a choice must be made between the child components. The symbol is a three-pole switch inside of a rounded box. The switch signifies that an author can choose either of the branches leading from the right edge. Because the borders of the box are dashed, the choice itself is optional. The “0..∞” symbol beneath the box means that the choice can be made multiple times.



Figure 9. Choice Symbol

Figure 10 shows the use of this symbol in context:

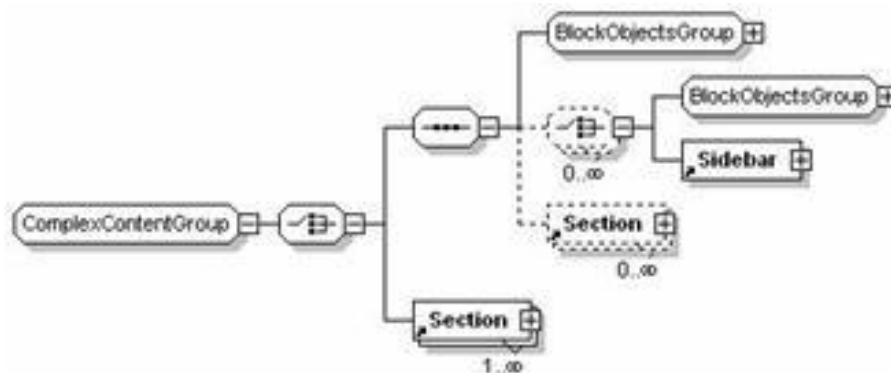


Figure 10. Sequence and Choice Combined

This schematic says that the grouping named **ComplexContentGroup** consists of a required choice between the top branch on the one hand and the bottom branch on the other. The top branch is a sequence of one element from the **BlockObjectsGroup**, optionally followed by a *repeatable* choice between **BlockObjectsGroup** elements and a **Sidebar** element, optionally followed by zero or more **Section** elements. The bottom branch leads to one or more **Section** elements.

H.5 Attributes

Elements may have properties. For example, the element **List** has the property called **listStyle**. In XML, such properties of an element are called *attributes* of the element. In the schematic diagrams used in this document, the attributes are displayed separately from the elements.

Appendix I Controlled Vocabulary Enumerations

The Controlled Vocabulary Enumerations (CVE) used in this DES are as follows:

Table 4. CVE Definitions

CVE File name	Definition	Attribute and Rules Cross Reference